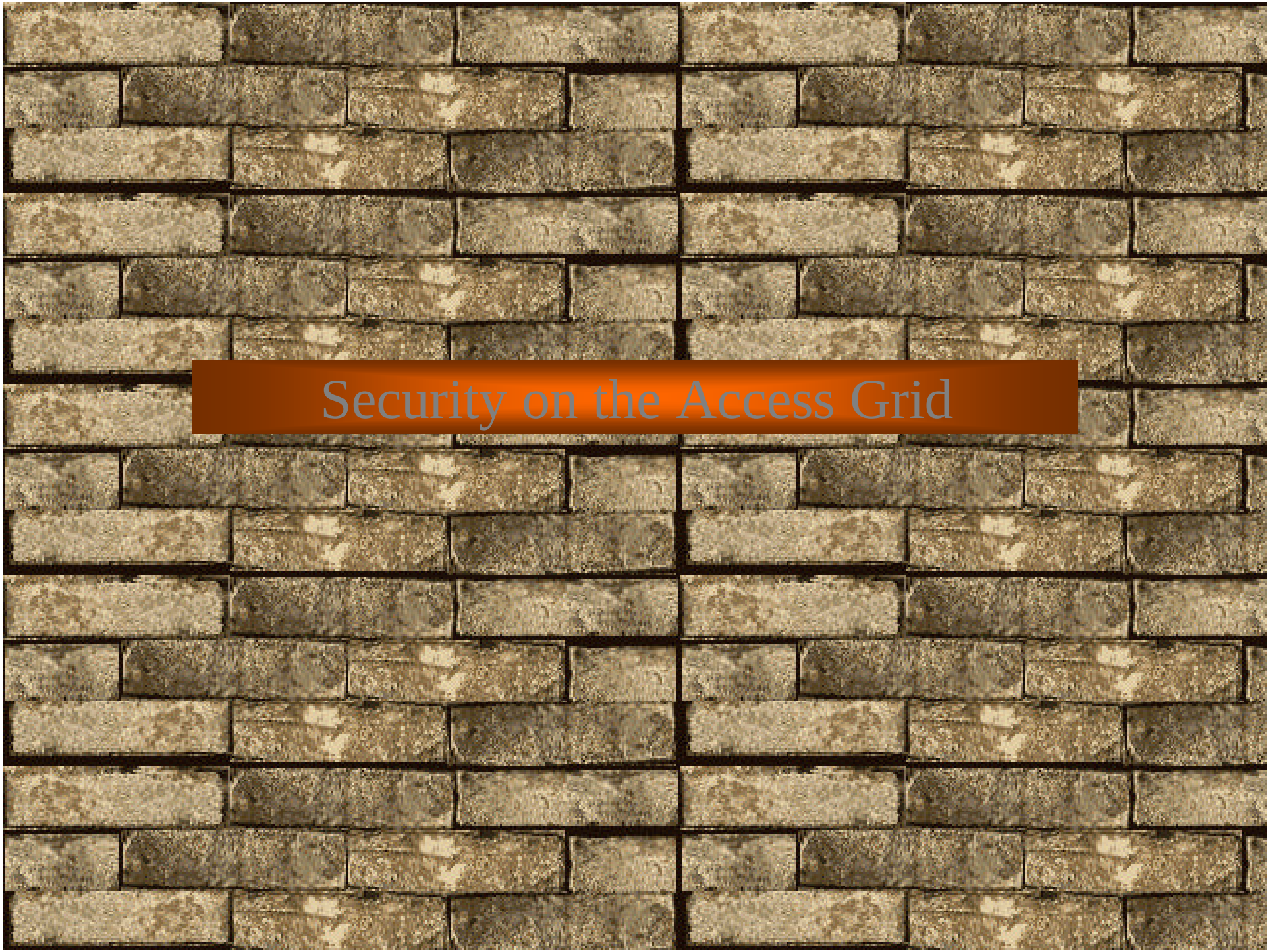
Security on the Access Grid

What does security mean?

- No one can hear our budget discussion
- I can tell exactly who is hearing our budget discussion
- I won't get fired if I use the Secure Access Grid
- I won't get fired, and I can blame Bob and Terry and Lisa if someone breaks in while I'm using the Secure Access Grid
- I can put my AG Node behind the department firewall and everything will be cool
- Everything is encrypted and password protected
- The script kiddies won't get me

FUTURESLAB

ACCESS GRID

AG Threat Model

- A threat model describes…
  - … attackers' resources
  - … what attacks are expected to be mounted
  - … what attacks we aren't going to worry about
- Assumptions
  - End systems not compromised
    - How to ensure this? (classical system intrusion detection mechanisms)
  - Attacker has complete control over communications channel
    - Steal packets
    - Generate packets
    - Forge packets

Passive attacks

- Attacker reads packets from the network
- Packet sniffing from shared LAN (Ethernet, wireless)
- Goal:
  - Obtain private information
  - Credentials
  - Passwords
  - Confidential data
  - Offline cryptographic attacks
- Multicast
  - Anyone can listen in!

Active attacks

- Spoofing attacks
- Denial of service
- Replay attacks
- Message insertion / deletion / modification
- Man in the middle
- Goals:
  - Disruption of service
  - Hijacking of data channels
  - For fun and profit

Social Engineering Attacks

- Strong encryption isn’t all there is
- “Hi,I lost my password, can you reset it and tell me what it is?”
- Security of passwords and private keys

What are we protecting in the Access Grid?

- Media streams
  - Audio
  - Video
- “Presentations”
  - PowerPoint
  - HTML slide shows
  - MPEG movies
  - Visualizations
- Node hardware
- System software
- Shared documents
  - Control streams
- Data
  - Nuke simulations
  - Design documents
  - Models
- Shared applications

From whom?

- Inadvertent lurkers
  - the abandoned node problem
- Over-interested third parties
- Everyone but those invited to private meetings
- Hackers intent on destroying our data
- Competitors

What if we're attacked?

- Do we need to prevent attacks?
  - We'd like to, if possible
- Is it sufficient to detect attacks?
  - It's certainly necessary
- How do we recover from an attack?
- To whom should we report attacks?
  - CERT analog for AG?

Requirements for a Security Architecture

- Confidentiality
- Message Integrity
- Endpoint Authentication
- Non-repudiation

- Discourage islands
  - Strong enough security to make the paranoid comfortable being connected to the world
  - Address users' comfort-level issues
- Systems Security
  - Unauthorized usage
  - Inappropriate usage
  - Denial of Service

FUTURESLAB

ACCESS GRID

How do we do this?

- *Identify* users and nodes
- *Authenticate* them with an authority we trust
- *Authorize* their access to the resources they request
- Provide them *privacy* and *secure access* to their applications and data

Identification, Authentication and Authorization

- Who am I?
- Who are you?
- Who can use the node? (local access)
- Who can use a virtual space? (venue access)
- Requirements:
  - Standards for naming of entities
  - Authentication mechanisms
  - Trusted authorities
  - Access control mechanisms (description and implementation)
  - Support for hardware identification tokens

Encryption and Privacy

- General mechanism:
  - Public key encryption for non-streaming media
  - Shared key encryption for streaming media
  - Session keys protected by public key encryption
- Who holds the keys?
- Current on physical and network security on Venues server

High-level Architecture

Community Server
Identity DB
Certificate Authority

Venue Server

Node

Node

Node

Venue Server

Venue Server

Node

Community Server

FUTURESLAB

ACCESS GRID

Proposed Instantiations

- Common naming architecture
  - LDAP Distinguished Names to identify users and nodes
- Authentication database
  - Maintained with LDAP database
  - OpenLDAP
  - iPlanet Directory Server
- Multiple authorization / authentication mechanisms
  - Strong crypto
  - Userid / Password
  - IP Source Address
- Authorization
  - Akenti mechanisms
- Certificate Authority
  - OpenSSL
  - iPlanet Certificate Management System
- Policy-based access control

Questions?

FUTURESLAB

ACCESS GRID